

REMARKS

The Office Action dated June 18, 2007, has been received and carefully considered. In this response, claims 1-5, 7, 8, 10, 11, 13-15, 19, and 20 have been amended. No new matter has been added. Entry of the amendments to claims 1-5, 7, 8, 10, 11, 13-15, 19, and 20 is respectfully requested. Reconsideration of the outstanding objections/rejections in the present application is also respectfully requested based on the following remarks.

I. THE INDEFINITENESS REJECTION OF CLAIMS 2, 7, 13, & 17

On page 3 of the Office Action, claims 2, 7, 13, and 17 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the invention. This rejection is hereby respectfully traversed.

The Examiner asserts that it is unclear from claims 2, 7, 13, and 17 whether the first and second mask values are different.

Claims 2, 7, 13, and 17 have been amended to address the Examiner's concerns.

In view of the foregoing, it is respectfully requested that the aforementioned indefiniteness rejection of claims 2, 7, 13, and 17 be withdrawn.

II. THE NON-STATUTORY SUBJECT MATTER REJECTION OF CLAIM 10 & 19

On pages 2-3 of the Office Action, claims 10 and 19 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. This rejection is hereby respectfully traversed.

The Examiner asserts that claims 10 and 19 are not directed to statutory subject matter. Applicant respectfully disagrees. However, in order to forward the present application toward allowance, Applicant has amended claims 10 and 19 to remove the language that the Examiner found objectionable and more specifically define the claimed invention.

In view of the foregoing, it is respectfully requested that the aforementioned non-statutory subject matter rejection of claims 10 and 19 be withdrawn.

III. THE ANTICIPATION REJECTION OF CLAIMS 1 & 8-11

On page 4 of the Office Action, claims 1 and 8-11 were rejected under 35 U.S.C. § 102(b) as being anticipated by Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient

Authenticated Encryption"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed invention. Id.

Regarding claim 1, the Examiner asserts that Rogaway discloses the claimed invention. Applicant respectfully disagrees for several reasons. First, the Examiner assumes that the first mask value and the second mask value as recited in claim 1 are equivalent values. This assumption is apparently

based upon the Examiner's interpretation of claims 2 and 7 as being unclear with respect to the first mask value and the second mask value. As discussed above, claims 2 and 7 have been amended to address the Examiner's concerns with respect to the first mask value and the second mask value. Thus, it is respectfully submitted that the first mask value and the second mask value as recited in claim 1 are not equivalent values. It should be noted, however, that, in certain circumstances (e.g., when computed to be the same based upon the computation factors as set forth in claims 2 and 7), the first mask value and the second mask value may have the same value.

Second, since the first mask value and the second mask value as recited in claim 1 should not be assumed to be equivalent as discussed above, it is respectfully submitted that Rogaway fails to disclose or even suggest the elements of whitening at least one message block with a first mask value, encrypting the at least one whitened message block using a block cipher and a first key, and whitening the at least one encrypted message block with a second mask value to generate at least one corresponding output ciphertext block, as claimed. In contrast, Rogaway discloses applying an identical offset $Z[i]$ to all but one string of a message M before and after a block cipher E_k (see pages 4-6).

Furthermore, Rogaway also discloses applying a string L and an offset $Z[m]$ to one string of a message M before a block cipher E_k , as well as applying the same message string $M[m]$ after the block cipher E_k (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

At this point Applicant would like to remind the Examiner that, as stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

At this point it should be noted that claim 1 has been amended for purposes of grammatical clarity only.

In view of the foregoing, it is respectfully submitted that claim 1 is allowable over Rogaway.

Regarding claims 8-11, these claims are dependent upon independent claim 1. Thus, since independent claim 1 should be allowable as discussed above, claims 8-11 should also be allowable at least by virtue of their dependency on independent claim 1. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, it is respectfully requested that the aforementioned anticipation rejection of claims 1 and 8-11 be withdrawn.

IV. THE OBVIOUSNESS REJECTION OF CLAIMS 2-7 & 12-20

On pages 5-9 of the Office Action, claims 2-7 and 12-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The Patent Office can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of references. Id. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). That is, under 35 U.S.C. § 103,

teachings of references can be combined only if there is some suggestion or motivation to do so. Id. However, the motivation cannot come from the applicant's invention itself. In re Oetiker, 977 F.2d 1443, 1447, 24 USPQ2d 1443, 1446 (Fed. Cir. 1992). Rather, there must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the art would make the combination. Id.

It is respectfully submitted that the aforementioned obviousness rejection of claims 2-7 has become moot in view of the deficiencies of the primary reference (i.e., Rogaway) as discussed above with respect to independent claim 1. That is, claims 2-7 are dependent upon independent claim 1 and thus inherently incorporate all of the limitations of independent claim 1. Also, the secondary reference (i.e., Schneider) fails to disclose, or even suggest, the deficiencies of the primary reference as discussed above with respect to independent claim 1. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference with the primary reference also fails to disclose, or even suggest, the deficiencies of the primary reference as discussed above with respect to independent claim 1. Accordingly, claims 2-7 should be allowable over the combination of the secondary reference with the primary reference at least by virtue of their

dependency on independent claim 1. Moreover, claims 2-7 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

Regarding claim 12, the Examiner asserts that the claimed invention would have been obvious in view of the combination of Rogaway and Schneier. Applicant respectfully disagrees for several reasons. First, the Examiner assumes that the first mask value and the second mask value as recited in claim 12 are equivalent values. This assumption is apparently based upon the Examiner's interpretation of claims 13 and 17 as being unclear with respect to the first mask value and the second mask value. As discussed above, claim 13 has been amended to address the Examiner's concerns with respect to the first mask value and the second mask value (claim 17 only recites a single mask value). Thus, it is respectfully submitted that the first mask value and the second mask value as recited in claim 12 are not equivalent values. It should be noted, however, that, in certain circumstances (e.g., when computed to be the same based upon the computation factors as set forth in claim 13), the first mask value and the second mask value may have the same value.

Second, since the first mask value and the second mask value as recited in claim 12 should not be assumed to be equivalent as discussed above, it is respectfully submitted that

Rogaway fails to disclose or even suggest the elements of applying a XOR function to all blocks of a message to compute a XOR-sum, applying a first mask value to the XOR-sum, encrypting the masked XOR-sum using a block cipher and a first key, and applying a second mask value to the encrypted XOR-sum to generate an integrity tag, as claimed. In contrast, Rogaway discloses applying an identical offset $Z[i]$ to all but one string of a message M before and after a block cipher E_k (see pages 4-6).

Furthermore, Rogaway also discloses applying a string L and an offset $Z[m]$ to one string of a message M before a block cipher E_k , as well as applying the same message string $M[m]$ after the block cipher E_k (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally, Rogaway also discloses applying an offset $Z[m]$ to a checksum before a block cipher E_k , and then limiting the block cipher result to a tag length τ (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally still, in contrast to the claimed invention, Rogaway also discloses applying and limiting as described above to a checksum of xor'ed message strings M , cyphertext string

C[m], and block ciphered string Y[m]. This disclosure by Rogaway clearly differs from the claimed invention.

Regarding combining Schneier with Rogaway to arrive at the claimed invention, such a combination would result in an inoperable methodology since replacing the limiting of Rogaway with an additional xor function as mentioned by Schneier would not result in a limited tag length τ , which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 12 is allowable over the combination of Rogaway and Schneier.

Regarding claims 13-20, these claims are dependent upon independent claim 12. Thus, since independent claim 12 should be allowable as discussed above, claims 13-20 should also be allowable at least by virtue of their dependency on independent claim 12. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

At this point Applicant would like to remind the Examiner that, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Also, as stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Further, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). Further, as stated in MPEP § 2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). That is, "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." In re

Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 2-7 and 12-20 be withdrawn.

V. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

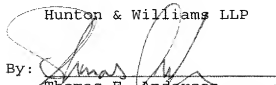
Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

U.S. Patent Application No.: 10/772,433
Attorney Docket No.: 57983.000164
Client Reference No.: 16404ROUS01U

Respectfully submitted,

Hunton & Williams LLP

By:


Thomas E. Anderson

Registration No. 37,063

TEA/vrp

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: September 12, 2007